VPN: 保證安全性與服務品質

林盈達、江美燕

摘要

近兩年來，以 VPN (Virtual Private Network) 相關技術發展企業網路已成為熱門話題，而安全性和服務品質的保證對於跨越公共網路的 VPN 顯得更形重要。本文將從企業網路的發展談起，包含租用專線及用 SMDS、ATM、Internet 等技術發展的 VPN，並比較這幾種用來發展企業網路的技術，在經濟、安全性及服務品質各方面的優缺點；接著把重心放在跨越 Internet 的 VPN 所面臨的問題與解決技術，以及相關的標準；最後，介紹並比較數種具代表性的 VPN 產品。

一. 前言

VPN (Virtual Private Network) 被譯做虛擬私有網路，正如其名，VPN 泛指各種架構於公共網路建設上的私有網路。如表一，Data Communications 雜誌在美國 Los Angeles、Houston、Boston 之間架設完全網狀連結(fully-meshed)，另有一條連結連至 London，每條連結均為 64kb/s，由購買 VPN 加密裝置、架設費用及第一年使用索費來看，相較於以往租用專線作為企業連結網路的方式，VPN 顯然佔了很大的經濟優勢，而這也是 VPN 興起最主要的原因，詳細說明請參看 [1]。

租用專線	FRAME RELAY VPN	INTERNET VPN
一年索費： $133,272 安裝： $2,700	一年索費： $89,998 安裝： $5,760 VPN 加密裝置 x4 $16,000	一年索費： $38,400 VPN 加密裝置 x4 $16,000
第一年總花費：$135,972	第一年總花費： $111,758	第一年總花費： $54,400

表一　租用專線與 VPN 花費比較

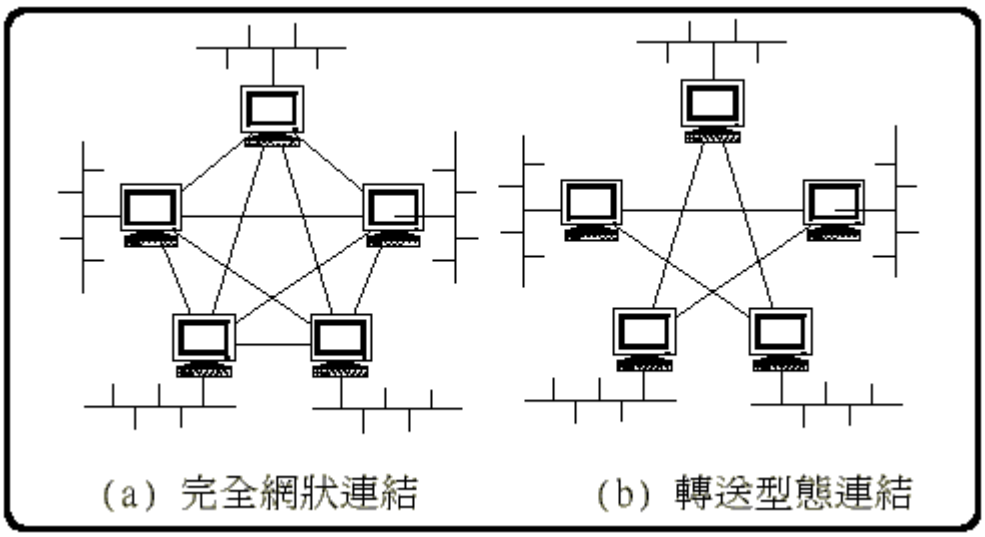
VPN 以架設於公共網路上的特質取得經濟優勢，然而，相較於以往租用專線的方式，VPN 也因此必須處理在公共網路上傳送資料的安全性問題，除了一般防火牆提供的收、發位址過濾，認證 (authentication)和加密 (encryption)也是確保 VPN 安全性重要的技術。所謂認證，就是確認欲進入企業網路的使用者或裝置為他們所宣稱的使用者或裝置；所謂加密，則是基於考量資料在公共網路傳送過程中可能被攔截、竊取的情形，因此將資料加密後再傳送，使竊聽者即使取得資料也無法解讀，相關技術和標準稍後將會做更深入的介紹、比較。

以 Internet VPN 而言，傳送的封包必須在公共網路上與其他封包爭奪網路資源，因此，為了達到形同私有網路的效果，VPN 必須考慮服務品質的問題。一方面考量整個 VPN 網路的服務品質(即 per-VPN Quality of Service)，另一方面則考量是否能讓在 VPN 上傳送的不同訊息得到不同等級的服務品質(即 per-flow Quality of Service)，這些問題與解決方案，事實上和各種公共網路本身能夠提供的服務品質有很大的關連性，待認識了企業網路的發展過程，並比較用各種技術模擬私有網路的優缺點後，應會有更深刻的體會。

二. 企業網路的發展

企業網路的發展起源於數個分公司間互相連結或供客戶存取公司資源的需求，為了維護企業網路內部資訊不被非法擷取，企業網路的安全，相較於一般公共網路，顯得更為重要；而企業對資料傳輸的品質要求，除了整體的保證外，對於不同性質的資料，可能也有不同的傳輸要求。接下來，我們便針對數種常見的企業網路技術，探討其安全性及所能提供的服務品質。

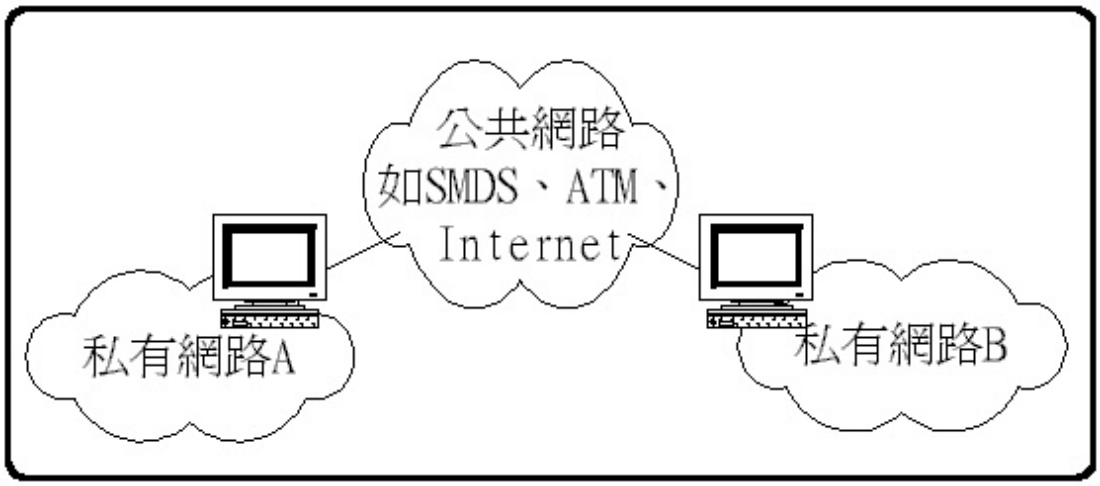
若企業網路與企業網路之間以租用專線的方式連結，如圖一(a)，假設某企業有 n 個分公司，欲租用專線連結各個分公司的企業網路，總共需要 C(n, 2)條專線以達到完全網狀連結；即使如圖一(b)，利用 router 轉送其他分公司的訊息，以減少專線數目，租用專線的花費依然十分驚人！而且以妥善運用網路資源的觀點來看，在專線負載量很低的時候，也不能將專線拿來做其他的運用，而此時租用費還隨著時間在計算著呢！不過，以服務品質保證的角度來看，租用專線作為企業網路，也就沒有 VPN 所面臨要和公眾網路上其他訊息爭奪網路資源的問題，在保證了整體服務品質後，對不同訊息提供不同服務等級的需求，則可由其他機制予以支援。



圖一　專線連結方式

結合了封包及細胞(cell)傳送的 SMDS (Switched Multi-megabit Data Service)

是第一個提供 VPN 服務的公眾數據服務網路（如圖二），SMDS 提供了點對點或點對多點的 datagram 傳送服務，利用 ITU (International Telecommunications Union)建議書 E.164 的起點及終點位址[2]，用戶可將送進來的資料阻隔，只接收從特定 SMDS 位址送出的資料(即 source address screening)，或是阻隔送出至特定 SMDS 的資料（即 destination address screening），藉由讓客戶選擇採全面開放式連結，或使用阻隔工具以達成緊密控制相關使用者團體，SMDS 提供了用戶連接到不同協定的區域網路的能力；在服務品質方面，SMDS 有項開放迴路流量控制機能，稱為 SIR (Sustained Information Rate)，採用信用管理(credit manager)或漏桶(leaky bucket)的管理方式，而其費用介於訊框傳送(frame relay)和 ATM 之間。



圖二　跨越公共網路的 VPN 架構圖

訊框傳送可用於封閉式使用者群組，達到 VPN 服務；且支援永久式虛擬電路（PVC）和交換式虛擬電路（SVC）的訊框傳送（frame relay），在傳送訊框時，若檢查出訊框有錯誤便將之丟棄，可有效的在低錯誤率的傳輸媒體上進行傳輸；在服務品質方面，訊框傳送定義了 CIR (Committed Information Rate)，指定網路在任何情況下必須提供的最小流量。隨著最近訊框傳送網路在加快速度、改善服務品質的進步[3]，其涵蓋範圍也大幅增加，雖然許多廠商有意願加強服務品質，但目前真正提供服務品質保證的廠商其實並不多。

將 VPN 架設於具有高速傳輸能力與服務品質保證的 ATM (Asynchronous Transfer Mode) 上聽起來是個不錯的想法！ 利用 VP (Virtual Path)和 VC (Virtual Channel) 的原理，ATM VPN 運作方式就像在大鐵路系統中租用數條鐵道線路的數個定時列車，用這數條線路連結各個企業網路，而資料便在這幾條線路間靠著 VP 交換機或 VC 交換機轉送。ATM VPN 的運作方式與租用專線的效果有些類似，自然保證了整個 VPN 連結的服務品質；另外，ATM 的 CIR (Committed Information Rate) 定義了使用者可送出訊框且網路保證會傳送的平均速率，可以針對各個資料流有不同的服務品質保證。雖然 ATM VPN 挾帶著上述傳輸能力與服務品質優勢，然而，過於複雜的運作，導致在技術上實行困難且價格昂貴，使它遲遲無法成為主流公共網路。

Internet 是現今應用最廣泛的公共網路，在 Internet 上提供 VPN 服務是許多人企求的解答。然而，TCP/IP 可說是沒有安全性可言，因此，除了先前提過的過濾收、發位址的方法外，各種認證(authentication)、加密(encryption)的技術也因應而生，為了幫助將來各家廠商、不同系統的 VPN 能夠整合，互相連結、傳送訊息，IETF (Internet Engineering Task Force) 定義了一套安全協定 IPSec (IP Security Group)，在下一個章節將會對各種認證、加密技術有更詳細的介紹。

如前所述，架設於公共網路上的 VPN 服務品質，實際上和所在公共網路本身的服務品質問題有很大的關連性，Internet VPN 也是如此。在 Internet 服務品質上的問題，有人提出了整合式服務(Integrated Service)的想法，運用 RSVP (ReSource reserVation Protocol)，盡量在每個路由器上預留頻寬，這樣的方式雖然對某些資料流有了傳送效率保證，但 RSVP 頻寬保留協定的複雜度能否使上千個資料流，在一台交換路由器上迅速被處理，是一大挑戰；後來，又有人針對 RSVP 這種整合式服務實行上的困難，提出了較為妥協的差別式服務(Differentiated Service)，不像 ATM 建連結，也不像整合式服務預留頻寬，而採行將封包分等級，例如依照對丟棄(loss)、延遲(delay)的容忍度分等級，而給予差別待遇，延伸出來的問題可能就是如何依照得到的服務品質收費了。

方式	安全性	服務品質	費用
租用專線	高	Per-VPN: 沒問題 Per-Flow: 需要其他機制支援	通常最高
SMDS VPN	可，依收、發位址過濾訊息	Per-VPN: 難 Per-Flow: 可藉 SIR 加強之	再次之
Frame Relay VPN	可，提供部份基本公眾網路安全能力	Per-VPN: 難 Per-Flow: 雖有 CIR 機制，但目前只有少部份服務提供者有服務品質保證	較低
ATM VPN	高	可透過 CIR 保證之 Per-VPN: VP 層次 Per-Flow: VC 層次	次高
Internet VPN	低，但可考慮 IP tunneling 相關技術	Per-VPN: 難 Per-Flow: 將來可考慮使用 Integrated Services 或 Differentiated Services	通常最低

表二　各種企業網路技術比較

三. Internet VPN 相關標準與技術

由於 Internet 是目前公共網路的主流，所以我們將討論重點放在 Internet

VPN。首先我們說明、比較各類 VPN 產品，然後針對在 Internet 上提供 VPN 所面臨最大的困難：安全問題，介紹各種認證、加密技術，其中包含 IP tunneling 的相關討論，並比較這些相關技術與現有的 Internet 安全技術，如 SSL、SET，和未來的 IPv6 協定的安全措施有何異同。

介於公共網路(如 Internet)與私有網路間的 VPN 產品基本上分成三大類：路由器(router)、防火牆、獨立的 VPN 裝置。

路由器通常將加密鑰匙存放在裝置內的矽晶體中，具有硬體設備速度快、不易被入侵的優點，有些廠商為了因應可能會有人直接闖入企業內部，奪取矽晶體上加密鑰匙的情況，便設計路由器在裝置殼子被非法打開時，自動迅速將矽晶體內的鑰匙毀掉，並通知安全人員處理。

防火牆的功能在於保證私有網路不會直接受到來自公共網路的攻擊，一般防火牆有兩種功能：Filter 防火牆和 Proxy 防火牆[4]，前者用以依 IP 過濾可以通過防火牆的訊息；後者則提供內部對外連結的轉接站，目前大部份的防火牆都合併了上述兩種功能。

這三種產品分別又可能是以軟體或軟硬體共同架構的系統，表三是以軟體或硬體架構 VPN 系統的優缺點比較，稍後會以各家產品為例，做更詳細的介紹、比較。

軟體	硬體
優點： ● 可以自動處理變更的資訊 ● 利於用不同管道來區分遠端存取資料的型態 缺點： ● 通常較難管理，必須熟悉作業系統、應用程式和安全機制 ● 受制於架構於其上的作業系統，通常必須再特別加強作業系統的安全性	優點： ● 較不易被直接破解入侵 ● 通常速度較快 缺點： ● 有些在每個終端工作站都需要有特殊的硬體（如 PC Card） ● 有些早期產品在每次網路拓蹼改變或使用者密碼被取消時，必須手動變更 ● 有些不管通訊協定為何，將所有資料作 tunnel

表三　軟體及硬體 VPN 裝置比較

由於 TCP/IP 無法保證安全性，因此 Internet VPN 的安全問題是很重要的議題。有一種將收、送位址和資料一同加密封包於內，並在封包外頭加上 VPN 裝置的位址，以類似挖掘了一個隧道的方式在 Internet 上傳送的技術，稱為 IP tunneling。隧道起始的位置有兩種可能，一種是在發送訊息的主機就將訊息封包起來，另一種則是在介於企業網路和公共網路間的 VPN 裝置才封包，主要差別取決於是否要對自己所在企業網路採取安全措施，即是否需要避免被企業網路內

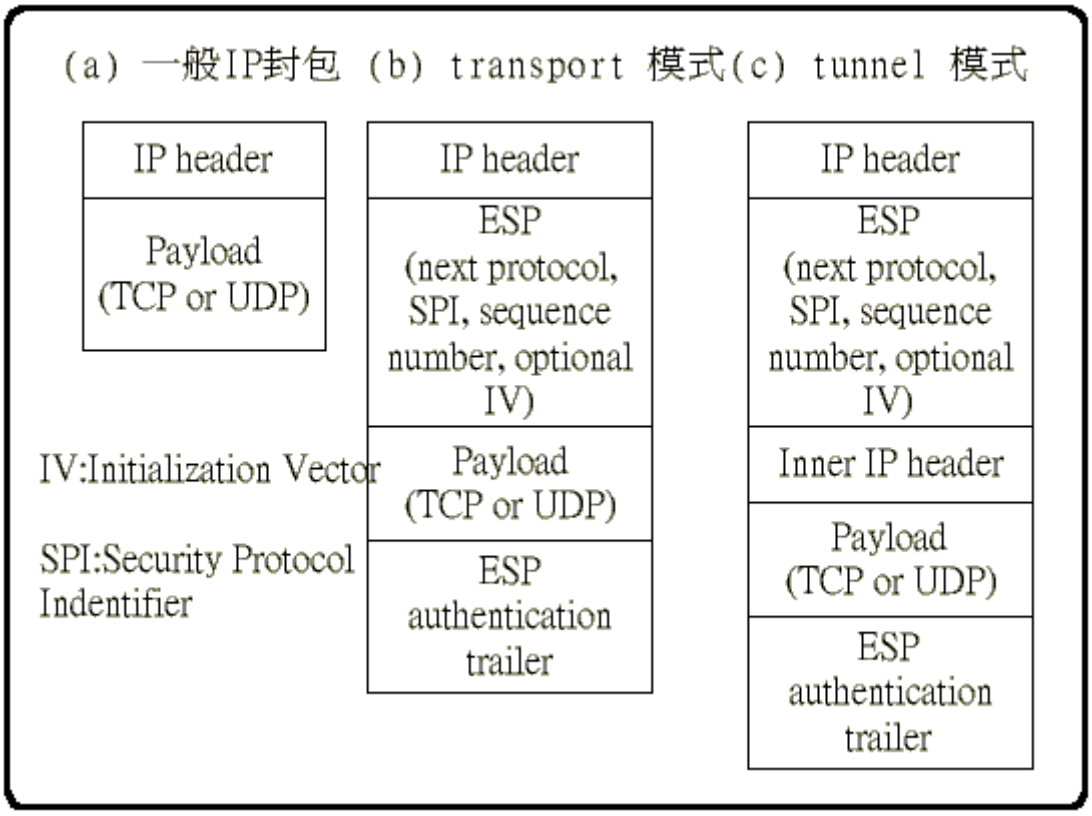
的其他成員得知資訊。目前能夠達到 IP tunneling 的技術紛雜，許多廠商甚至自行研發技術，造成現今大部份互相連結的網路，其對等的 VPN 裝置必須相同，才能溝通，其中較常見的 IP tunneling 技術有 IP Sec、PPTP 和 L2TP。

PPTP (Point-to-Point Tunneling Protocol)是由 Microsoft 和 Ascend 共同發展，主要支持廠商有 Bay、Indus River、3Com，屬於 OSI 架構中第二層，用以封包任何第三層的協定，在認證、加密和鑰匙管理上都沒有指定標準。

L2TP (Layer 2 Tunneling Protocol)混和了 PPTP 和 Cisco 的 L2F (Layer 2 Forwarding) ，和 PPTP 一樣用來封包第三層的協定，也同樣沒有指定認證、加密和鑰匙管理的標準，主要支持廠商有 Bay、IBM、Onebox、Xyplex Network 等。

IPSec (IP Security group) [5]是 IETF (Internet Engineering Task Force)為了促進未來不同 VPN 裝置間連結、溝通所訂定，也是目前聲望最高的技術標準，一共分成三大部份：ESP、AH、ISAKMP。

ESP (Encapsulation Security Payload)[6]提供認證和加密，其中認證為選擇性的，如圖三，ESP 將一般 IP 封包(a)以 DES 或 Triple DES 加密之後， 就形成(b)或(c)的格式，如前所述，依照對企業網路內部是否採取安全措施，可以選擇以發送訊息的主機或 VPN 裝置為隧道起始點，(b)中的 transport 模式是 IPSec 在主機上發生的結果，負載物(payload)的部份也就是原來跟著 IP header 的部份，並未做修改，所以稱為 transport 模式；若 IPSec 發生的地方是在內、外網路之間的路由器、防火牆或 VPN 閘道，負載物的部份就會是原來終端使用者完整的封包，原來的整個封包通過一個隧道傳送到 TCP/IP 網路的另一端，如(c)，因此稱為 tunnel 模式。



圖三　ESP 封包示意圖

AH (Authentication Header) [7]只提供認證的動作，通常是靠 MD5 (Message Digest 5)、SHA1 (Secure Hash Algorithm 1) 或者發展中的 HMAC (Hashed Message Authentication Code)來確認使用者的身份。由於 ESP 和 AH 加密的動作都會使封包變大，可能因而超過封包規定大小，此時有兩種處理方式：將之分成兩個封包，或者通知送端無法處理。

ISAKMP (IP Security Association Key Management Protocol) [8]使交換鑰匙的動作自動化，並確定它們從一端安全地送至網路另一端。

其實在 VPN 開始發展之前，Internet 就已經陸續發展出一些加強安全性的協定，像是 SSL (Secure Sockets Layer)、SET (Secure Electronic Transactions)等，而被視為下一代網際網路協定的 IPv6，也在它 128 bits 長的封包中（目前使用的 IPv4 為 32 bits）加入了控制加密動作的位置，也就是可以在 IP 層進行加密，即 IP tunneling，目前 IPSec 已開始支援 IPv6 的安全特性。

究竟 SSL、SET 和我們這裡提到的 IPSec 有何差異呢？最主要的差異在於進行安全措施相對應於 OSI 架構的層次不同，以及應用範圍不同，詳細資料如表四。

技術	進行層次與方式	應用範圍
IPSec	在第二層加密第三層的封包	VPN
SSL	Session 層，在兩個應用程式間提供隱	常用於 Web，也可用於 e-mail、ftp、

	私且可靠的連結，保證連結被確認，而非對傳送的文件本身加密	telnet 等應用程式
SET	Application 層	主要用於 Internet 上的信用卡交易

表四　各種 Internet 上安全技術比較

四. 產品現況

VPN 裝置產品眾多，唯一的共同點是：它們都對使用者進行認證，且將傳送於端點間的資料流予以加密。相異的地方包括使用軟體或者軟硬體混合；只有認證及加密功能，或者還包含路由器及防火牆的存取控制功能；支不支援 IPSec；各種認證方法，如標記認證卡(token authentication cards)、Radius 伺服器、真實字母加密(a veritable alphabet soup of encryption algorithm)等；VPN 型態為 client-server 或 server-to-server。

為了瞭解 VPN 產品現況，我們選擇在 Data Communications 雜誌測試實驗室中脫穎而出的幾種產品做介紹，詳細測試方法，以及其他產品的測試比較請參看[9][10]。

表五列出的是在安裝與管理容易度上表現較出色的四種產品，Check Point 的 Firewall-1 在簡易安全管理上表現出色，安裝防火牆時圖形化的介面也延伸至 VPN 中； 相較於其他產品迫使使用者在檢查或更改參數時，必須經過多個選單的不便，Isolation Systems 的 Infocrypt Enterprise 將所有裝置和 VPN 隧道相關訊息展示於同一畫面，更易於管理；Sun 的 Sunscreen EFS 採 Windows 95 用戶端軟體，使 VPN 安裝過程簡化至只需選擇一個防火牆，配予適當的證明權狀(certificate)；Timestep 的 Permit Security Gateway 簡化了認證權狀的使用，可將許多參數輸入裝置，節省了大量時間。

廠商	CHECK POINT SOFTWARE TECHNOLOGIES LTD.	SUN MICROSYSTEMS INC.	ISOLATION SYSTEMS LTD.	TIMESTEP CORP.
軟硬體	只有軟體	只有軟體	軟硬體混合	軟硬體混合
產品	Check Point Firewall 1 3.0	Sunscreen EFS1.1	Infocrypt Enterprise	Permit Security Gateway
拓蹼形狀	Server-to-server Client-server	Client-server	Server-to-server Client-server	Server-to-server Client-server
防火牆整合	Yes	Yes	No	No
認證	MD5, S-Key SecurID,Zxent	SKIP	MD5, PAP, CHAP, Radius,	MD5, certificates,

			SSL3.0, SecurID	passwords
加密	IPSec, DES, Triple DES	RC2, RC4, DES, Triple DES	IPSec, DES, Triple DES	DES, RCA
鑰匙管理	ISA/KMP, SKIP, FWZ, manual IPSec	SKIP	Digital certificates, Diffie-Hellman	Timestep Security Association Protocol
Tunneling	PPTP, L2TP, L2F	SKIP	Isolation Tunneling	None
價格（server 及 100 connections）	$18,990	$4,995	$9,950	$32,850

表五　易於安裝與管理的 VPN 產品

表六列出的是在嚴苛測試中，執行效能較好的兩種產品，Radguard 公司的 ciPro-VPN 提供了相當好的安全防護，其 CA(Certificate Authorities)及管理軟體使它相當容易設定，且可監控大量 VPN 使用者；VPNet 公司的 VSU 1010 在高速 VPN 效能評估中表現甚佳，在壓力測試中表現最佳，且提供了直覺、有用的監控工具，及針對遠端管理的安全通道。

廠商	RADGUARD INC.	VPNET TECHNOLOGIES INC.
產品 / 測試軟體版本	ClPro-VPN / 3.05	VSU 1010 / 2.0
防火牆 / IP 路由器	Yes / Yes	No / Yes
加密	DES, triple DES	DES, triple DES
鑰匙管理	IKE draft version 9	IKE draft version 9, SKIP
認證	Integrated 或 external CA, token authentication cards	External CA, CHAP, Radius, token authentication cards
Client 軟體	Windows95, Windows NT 3.51, Windows NT 4.0	Windows95, Windows NT 4.0
每個 Client 價格	$100	$99 (1 user) to $22 (600 or more users)

每個 VPN 裝置價格	VPN: $5,950 CA: $5,950	$4,995 (2 interfaces)

表六　效率較好的 VPN 產品

五. 結論

相較於所費不訾的租用專線方式，跨越公眾網路的 VPN 服務顯然是另一個企業網路發展的大好途徑。欲發展一個 VPN 企業網路，從一開始選擇所要跨越的公眾網路，接著面對各個已標準化或未標準化的安全協定，以及各種繁雜 VPN 產品，實是一件不容易的事，最後，我們就幾個架構 VPN 網路的考慮因素[11] ，作一番分析。

- 企業網路的拓蹼形狀
  一般來說，拓蹼形狀愈是接近星狀(即 hub-and-spoke)，愈適合使用訊框傳送、ATM 等網路，因為這樣較易管理；而網狀的最好採用 Internet，如果使用訊框傳送或 ATM，可能會面臨路由表過於複雜，管理不易，且需佔用許多 PVC 的問題。
- 單一或多種協定的網路
  使用多種協定的企業網路，由於在 IP 上採用的加密方法可能不同，額外負擔會很大；相較之下，訊框傳送或 ATM 就較適合。
- 客戶連結頻繁與否
  若客戶要連結進企業網路，訊框傳送或 ATM 便得花時間建 VPC，而路由表變更，管理也會變得更複雜，而且很難阻隔客戶在企業網路內的行動，可能對企業網路的安全造成威脅；若採行 IP，一則不需花建立 VPC 的時間，另一則可以藉路由器做到分區，增加效率與安全性。
- 對服務品質的要求
  一般來說，訊框傳送或 ATM 因為有 CIR 指定服務品質的功能，因此不論是對整個 VPN 連結或單一資料流的服務品質要求，都勝過 IP。

參考資料

[1] Andrew Cray, “Secure VPNs , Lock the Data, Unlock the Savings”, Data Communications, May 21, 1997

[2] CCITT Recommendation E.164, “Numbering Plan for the ISDN Era”, Vol, II. Fas.II.2, Blue Book, ITU, 1998

[3] David Greenfield, “International Improvements”, Data Communications , August,1998

[4] Mark Grennan, “Firewalling and Proxy Server HOWTO” markg@netplus.net v0.4, 8 November 1996

[5] Stephen Kent, Ran Atkinson, “Security Architecture for the Internet Protocol”,

August 5,1998

[6] Stephen Kent, Ran Atkinson, “IP Encapsulating Security Payload (ESP) “, July 6,1998

[7] Stephen Kent, Ran Atkinson, “IP Authentication Header”, July 6,1998

[8] D.Maughan, M.Schertler, M.Schneidor, J.Turner, “Internet Security Association and Key Management Protocol (ISAKMP)”, July 10,1998

[9] Deval Shah, Helen Holzbaur, “VPNs: Security With an Uncommon Touch” , Data Communications, September 21, 1997

[10] David Newman, Tadesse Giorgis, Farhad Yavari-Issalou, “VPNs: Safety First, But What About Speed?” , Data Communications, July, 1998

[11] Robin Gareiss, “Frame Relay vs. IP: It’s Your Move”, Data Communications, February , 1997